

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-v-

RAZHDEN SHULAYA, et al.

Defendants.

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #: _____
DATE FILED: December 20, 2017

17-cr-0350 (KBF)

OPINION & ORDER

KATHERINE B. FORREST, District Judge:

On June 7, 2017, Razhden Shulaya, Zurab Dzhnashvili, and thirty-one others were charged with a variety of racketeering, fraud, narcotics, firearms, and stolen property offenses; many, including Shulaya and Dzhnashvili, were arrested on the same day. The defendants—most of whom were born in the former Soviet Union and maintain substantial ties to Georgia, the Ukraine, and Russia—are alleged to be members of the “Shulaya Enterprise,” an organized criminal group under Shulaya’s command. According to the Indictment, the Enterprise is based in New York City but runs operations throughout the United States and abroad. The activities described in the Indictment include, inter alia, illegal gambling, extortion of those who owed debts to the Shulaya Enterprise, trafficking in contraband cigarettes and stolen merchandise, efforts to defraud casinos, identity theft, and use of violence.

Defendants are charged with: racketeering conspiracy; conspiracy to sell and transport stolen goods; conspiracy to traffic contraband tobacco; conspiracy to

commit fraud relating to identification documents; wire fraud conspiracy; narcotics conspiracy; and obstruction of justice.

Pending before the Court is a series of pretrial motions seeking suppression of evidence (based on purportedly improper communications interceptions and geolocation tracking), dismissal of Count IV, and routine pretrial disclosures. (See generally ECF Nos. 385, 388, 389, 391, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 413, and 420.) None of the motions requires resolution of a disputed issue of fact and thus the Court has not held an evidentiary hearing.

Zurab Dzhnanashvili has moved to suppress the Title III Orders on the theory that the Government's application did not sufficiently demonstrate that other investigative techniques were inadequate. (ECF No. 387, Mem. of Law in Supp. of Def. Zurab Dzhnanashvili's Pretrial Mots. ("Dzhnanashvili Mem.") at 9–20.) Alex Mitselmakher has also moved to suppress the Title III Orders, arguing that the district court lacked "territorial jurisdiction to authorize the wiretaps." (ECF No. 390, Mem. of Law of Alex Mitselmakher in Supp. of His Mot. to Suppress Intercepted Conversations ("Mitselmakher Mem.") at 2.) Ivan Afanasyev has moved to suppress location information gathered about his cellphone, for a bill of particulars, for early disclosure of witness identities and Rule 404(b) evidence, and for an order requiring the Government to abide by its Brady obligations. (ECF No. 392, Mem. of Law in Supp. of Def. Ivan Afanasyev's Pretrial Mots. ("Afanasyev Mem.") at 2.) Vache Hovhannisyan has moved to dismiss Count Four as duplicitous and for a bill of particulars. (ECF No. 402, Mot. to Dismiss Count Four, For Bill of

Particulars, and for Leave to Join Co-Defendant's Motions ("Hovhannisyan Mem.") at 3–6.)

In addition, seventeen defendants (including those mentioned above) purport to join in all motions. (See ECF Nos. 385 (Zurab Dzhanashvili), 389 (Alex Mitselmakher), 391 (Ivan Afanasyev), 394 (Nazo Gaprindashvili), 395 (Denis Savgir), 396 (Mikheil Toradze), 397 (Diego Gabisonia), 398 (Azer Arslanouk), 399 (Giorgi Lomishvili), 400 (Erekle Kereselidze), 401 (Zurab Buziashvili), 402 (Vache Hovhannisyan), 403 (Akaki Ubilava), 404 (Andriy Petrushyn), 405 (Levan Makashvili), 406 (Artur Vinokurov), and 420 (Bakai Marat-Uulu).)

For the reasons set forth below, the Court DENIES each of the pending motions.

I. BACKGROUND

A. Factual Background

The following statement of facts is drawn from the parties' submissions.

In the summer of 2014, agents with the Federal Bureau of Investigation ("FBI") began investigating a criminal group based in New York City. (ECF No. 388-1, Aff. in Supp. of Application for Order Authorizing the Interception of Wire Commc'ns Over a Cellular Tel. ("December Aff.") at 16.) The FBI believed that the group was controlled by a "vor v zakone," or a "Thief-in-Law," who stands at the highest level of Russian organized criminal groups, akin to a "Godfather" within an Italian organized criminal group. (Id. at 16–17.) According to the FBI, Razhden Shulaya acts as such a vor for what has been termed the "Shulaya Enterprise," and

thus oversaw subordinates who participated in criminal activities with his permission and for his benefit in exchange for protection, and who enforced his authority through intimidation and violence. (Id. at 17–18.)

The FBI deployed a range of techniques in investigating the Shulaya Enterprise. For example, they made controlled sales of purportedly stolen cigarettes, conducted stakeouts, and used an undercover officer. (See, e.g., id. at 18–25.) They also used confidential sources and obtained recordings of Shulaya and others through body recording devices and over consensually recorded telephone lines. (See, e.g., id. at 18–19, 25–29, 35.) In addition, they collected pen register, telephone toll data, and bank records and spoke to victims in the community. (See, e.g., id. at 29–30, 34, 43–47.)

By fall 2016, the FBI had evidence that the Shulaya Enterprise had, among other things, operated an underground poker room, extorted debtors, and purchased and sold untaxed cigarettes. The FBI had also uncovered evidence that the Shulaya Enterprise was planning to defraud casinos in Atlantic City. Despite the investigative success to that point, the full scope of the Shulaya Enterprise’s activities, its financing, and its complete membership remained unknown. (See id. at 7 (discussing objectives of the interception).)

In December 2016, following almost eighteen months of other investigative work, the FBI began intercepting wire and electronic communications of various members of the Shulaya Enterprise. At various points, the FBI intercepted calls to and from telephones used by Razhden Shulaya, Zurab Dzhanashvili, and Nazo

Gaprindashvili. The communications were monitored from wirerooms in Manhattan, New York. (See id. at 12; ECF No. 388-2, Aff. in Supp. of Application for Order Authorizing the Interception of Wire Commc'ns Over a Cellular Tel. ("January Aff.") at 13; ECF No. 388-3, Aff. in Supp. of Application for Order Authorizing the Interception of Wire Commc'ns Over a Cellular Tel. ("February Aff.") at 14; ECF No. 388-4, Aff. in Supp. of Application for Order Authorizing the Interception of Wire Commc'ns Over a Cellular Tel. ("March Aff.") at 15; ECF No. 388-5, Aff. in Supp. of Application for Order Authorizing the Interception of Wire Commc'ns Over a Cellular Tel. ("April Aff.") at 15; ECF No. 422-7, Aff. in Supp. of Application for Order Authorizing the Interception of Wire Commc'ns Over a Cellular Tel. ("May Aff.") at 15.)

The FBI acted pursuant to authority conferred by six consecutive judicial orders of interception:

1. An initial order of interception was signed on December 12, 2016, by the Hon. Katherine Polk Failla. The December 12 Order permitted the interception of wire communications occurring over the cellular phones initially identified as 929-247-6909 (the "Shulaya 6909 Phone"), 201-887-7880 (the "Shulaya 7880 Phone"), 347-571-1345 (the "Zura Phone"), and 941-224-8643 (the "Anna Phone"). (Thomas Decl. ¶ 4.)
2. A second order of interception was signed on January 12, 2017, by the Hon. Lewis A. Kaplan. The January 12 Order authorized continued interception of wire communications over the Shulaya 6909 Phone, the

Shulaya 7880 Phone, and the Zura Phone. The January 12 Order further authorized the initial interception of electronic communications over the Shulaya 7880 Phone and the Zura phone, as well as the initial interception of wire communications (but not electronic communications) over the cellular telephone initially identified as 929-355-2477 (the “Shulaya 2477 Phone”). (Id. ¶ 5.)

3. A third order of interception was signed on February 10, 2017, by the Hon. Paul A. Engelmayer. The February 10 Order authorized the continued wire and electronic interception over the Zura phone; continued wire interceptions over the Shulaya 6909 Phone and the Shulaya 7880 Phone; and authorized initial electronic interceptions and continued wire interceptions over the Shulaya 2477 Phone. (Id. ¶ 6.)
4. A fourth order of interception was signed on March 10, 2017, by the Hon. Denise Cote. The March 10 Order authorized the continued wire and electronic interception over the Zura Phone and the Shulaya 2477 Phone and continued wire interceptions over the Shulaya 6909 Phone and the Shulaya 7880 Phone. (Id. ¶ 7.)
5. A fifth order of interception was signed on April 7, 2017 by the Hon. George B. Daniels. The April 7 Order authorized the continued wire and electronic interception over the Zura Phone and the Shulaya 2477 Phone and continued wire interceptions over the Shulaya 6909 Phone and the Shulaya 7880 Phone. (Id. ¶ 8.)

6. A sixth order of interception was signed on May 17, 2017 by the Hon. Loretta A. Preska. The May 17, 2017 Order authorized continued interception of wire communications over the Shulaya 6909 Phone and the Shulaya 7880 Phone, and the interception of both wire and electronic communications over the Shulaya 2477 Phone and the Zura Phone. (Id. ¶ 9.)

Each of the Title III Affidavits described various investigative techniques deployed by the FBI up to that point, the limitations of those techniques, and the need for interception to satisfy outstanding investigative goals. (See December Aff. 47–54; January Aff. 70–79; February Aff. 42–53; March Aff. 51–63; April Aff. 61–75; and May Aff. 59–73.) In each of the Title III Orders, the authorizing judge found that the Government had demonstrated adequately that normal investigative techniques had been tried and failed, were reasonably thought to be unlikely to succeed, or were too dangerous to attempt. (See ECF No. 422-1, December 12 Order of Interception at 6; ECF No. 422-2, January 12 Order of Interception at 7; ECF No. 422-3, February 10 Order of Interception at 8; ECF No. 422-4, March 10 Order of Interception at 8; ECF No. 422-5, April 7 of Interception Order at 8; ECF No. 422-6, May 17 Order of Interception at 8.) Interception pursuant to the Title III Orders revealed that the Shulaya Enterprise was pursuing a range of criminal activities, that its leaders were in contact with criminal authorities in other cities and in other countries, and that the Enterprise was committing fraud in cities around the United States. (Compare December Aff. 5–7 with May Aff. 7–10, 43–44.)

On or about May 31, 2017, the Government sought a warrant and order for prospective location information for approximately seventeen different cellphones believed to be used by approximately seventeen different target subjects. (See generally ECF No. 391-4, Agent Aff. in Supp. of Warrant and Order for Cellphone Location and Pen Register Info., No. 17 Mag. 4107 (“GPS Aff.”).) The Hon. Katharine H. Parker, U.S. Magistrate Judge, issued the requested warrants, including a warrant for a cellphone believed to be used by Afanasyev. (See ECF No. 391-1, Warrant and Order for Cellphone Location Info. and Pen Register Info. And for Sealing and Non-disclosure (“GPS Warrant”).) This warrant allowed the FBI to access Afanasyev’s precise location for 45 days—though only five days were in fact monitored—and to access stored cell site records for the five days preceding May 31, 2017. (Id.; see Thomas Decl. ¶ 12.)

The GPS Affidavit included specific allegations about the Shulaya Enterprise’s identity fraud and cargo theft schemes. (GPS Aff. ¶¶ 11-19.) For example, it identified Afanasyev’s and Hovhannisyan’s cellphones as having been used in the counterfeit credit card and forged check schemes as well as Afanasyev’s involvement in a scheme to deliver and sell stolen goods. (Id. at 23 n.14; id. ¶¶ 15, 19(c).) The FBI began collecting location information pursuant to the GPS Warrant on or about June 2, 2017. (See ECF No. 422, Thomas Decl. ¶ 13.)

On or about June 6, 2017, a grand jury returned an indictment charging twenty-six members and associates of the Shulaya Enterprise. (See ECF No. 1, Sealed Indictment). In subsequently unsealed superseding indictments, the grand

jury charged additional persons. (See ECF. Nos. 58 (Khurtsidze), 189 (Marat-Uulu and Jikia).)

The grand jury charged Zurab Dzhnanashvili in four counts: racketeering conspiracy, conspiracy to transport and sell stolen goods, conspiracy to distribute untaxed cigarettes, and identity fraud conspiracy. (See ECF No. 1 ¶¶ 6, 9 (racketeering), 12–14 (stolen goods), 16–17 (cigarettes), 19–24 (identity fraud).) Ivan Afanasyev and Vache Hovhannisyan were also charged in the racketeering conspiracy and the identity fraud conspiracy. (See ECF No. 1 ¶¶ 9, 19–24.) Mitselmakher was charged only in the identity fraud conspiracy. (See ECF No. 1 ¶¶ 19–24.) The identity fraud conspiracy—Count Four of the Indictment—alleges that Dzhnanashvili, Afanasyev, Hovhannisyan, and Mitselmakher violated 18 U.S.C. § 1028(f). (See ECF No. 1 ¶¶ 19–24.) That conspiracy had multiple objectives related to the creation, transfer, and use of unlawful identification documents. (See ECF No. 1 ¶¶ 18-24.) Of relevance here, the grand jury charged both Afanasyev and Hovhannisyan with agreeing to each of the conspiratorial objects.

Agents with the FBI arrested Dzhnanashvili, Mitselmakher, Afanasyev, Hovhannisyan, and many of the other defendants on or about June 7, 2017. That same day, the Government ceased Title III interceptions pursuant to the May 17 Order and ceased collecting cellphone location data pursuant to the GPS Warrant. (See Thomas Decl. ¶ 9.)

Starting on or about June 27, 2017, the Government began producing discovery material to the defendants. Within approximately one month following

the defendants' arrests and presentments, the Government produced all affidavits and legal process in support of the series of Title III Orders obtained in the course of the investigation; affidavits and warrants pertaining to various search electronic mail accounts, collected geolocation data, searched physical premises; draft transcriptions and line sheets of Title III interceptions, consensually recorded calls, and in-person meetings; surveillance video and photographs; pen register data; subpoena returns (including telephone subscriber information, bank records, and other business records); and photographs of the content of certain electronic devices and computers, including screenshots pertaining to software programs used to conduct the casino scheme charged in the Indictment. Meanwhile, the FBI processed and reviewed electronic devices collected at the time of the defendants' arrests. That process is nearing an end, and the Government has represented that it is copying the content of those devices to storage media provided by the defendants and will make this tranche of discovery available before the end of this year.

Among the first documents provided in discovery were the Title III Affidavits. The final such affidavit, the May Affidavit, totaled approximately 77 pages in length and incorporated each of the prior affidavits. As such, the May Affidavit alone provides well over 200 pages of narrative description and analysis of the Shulaya Enterprise's composition and activities. That affidavit specifically discussed the operation of the Shulaya Enterprise's poker house, its cargo theft scheme, its contraband cigarette distribution, its various identity theft schemes (including the

cargo theft and other credit card and check-based frauds), extortions, violence, and the casino fraud. The May Affidavit and its attachment provides a detailed, narrative description of each of those offenses, and of the various defendants' (and other co-conspirators') roles in those offenses, much of which is directly incorporated into the overt acts set forth in the Indictment.

On June 9, 2017, the Court held an initial pretrial conference during which the Government set out a lengthy summary of the case. That summary also included a description of the various schemes charged in the original indictment, as well as a detailed summary of the evidence collected in the course of the Government's investigation. The following week, on June 16, 2017, the Court held a conference at which the bail conditions previously imposed for defendant Hovhannisyan in the district of his arrest, were appealed by the Government. In advance of that conference, the Government submitted a letter proffering facts regarding the fraudulent schemes in which Hovhannisyan and others (including, principally, Dzhanashvili, Afanasyev, and Savgir) had been involved. That proffer included quotations from draft line sheets obtained via the Title III intercepts described above, as well as summaries of surveillance, emails exchanged between defendants, and the Government's interpretation of key events and communications involving the defendants described in that letter. On July 26, 2017, the Government submitted a substantially similar letter in connection with a bail application by Savgir. That letter further included a description of various cardmaking equipment and devices found in Savgir's home as the result of a search

warrant executed on those premises. On August 9 and 28, 2017 the Government submitted similar bail letters regarding in advance of bail and detention hearings requested by Shulaya and Gabisonia, respectively. Each of these letters has set forth detailed discussions of the respective defendant's roles and criminal conduct.

II. SUPPRESSION MOTIONS¹

A. Legal Principles

1. Intercepted Communications

18 U.S.C. § 2518(3) allows a judge to “enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction).” The statute defines “intercept” as the “aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” Id. § 2510.

When reviewing a Title III application, a court must determine that there was probable cause to believe that (a) an individual was committing, had committed, or is about to commit a specified crime, (b) communications concerning that crime would be obtained through the wiretap, and (c) the facility (here, cell

¹ The burdens of production and persuasion generally rest upon the movant in a suppression hearing. United States v. Arboleda, 633 F.2d 985, 989 (2d Cir. 1980). “The movant can shift the burden of persuasion to the Government and require it to justify its search, however, when the search [is] conducted without a warrant.” Id.

phones) to be wire tapped was being used for criminal purposes or was about to be used or owned by the target of the wiretap. See id. § 2518(3); United States v. Yannotti, 541 F.3d 112, 124 (2d Cir. 2008) (citing United States v. Diaz, 176 F.3d 52, 110 (2d Cir. 1999)) (stating the same standard). In determining whether there is a sufficient basis to support finding probable cause, a court examines the “totality of the circumstances” and ask whether those circumstances reflect the fair probability that evidence of a crime will be found. Illinois v. Gates, 462 U.S. 213, 238 (1983). Courts are to use a practical, common sense approach. Id. In reviewing a suppression motion regarding a Title III application, a court is not undertaking a de novo review: it should give considerable deference to the judge who authorized the wiretap. United States v. Concepcion, 579 F.3d 214, 217 (2d Cir. 2009) (noting that the appellate court grants “considerable deference to the district court's decision whether to allow a wiretap”); see also Yannotti, 541 F.3d at 124; Diaz, 176 F.3d at 110.

i. Necessity

A Title III application for interception of telephonic communications must include, inter alia, a statement as to whether or not other “investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.” 18 U.S.C. § 2518(1)(c); id. § 2518(3)(c). In other words, interception should occur only when there is “a genuine need for it and only to the extent that it is needed.” Dalia v. United States, 441 U.S. 238, 250 (1979). However, it is not necessary to exhaust any or all other investigative procedures

before a wiretap may be authorized; rather, a court should view an application in light of practicality and common sense. Diaz, 176 F.3d at 111 (noting also that the statute “only requires that the agents inform the authorizing judicial officer of the nature and progress of the investigation and of the difficulties inherent in the use of normal law enforcement methods” (internal quotations omitted)).

ii. Territorial Jurisdiction

As noted above, a judge may authorize interceptions “within the territorial jurisdiction of the court in which [he/she] is sitting.” 18 U.S.C. 2518(3). The statute does not, however, “specify precisely where an interception is deemed to occur.” United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992). While an “interception” does occur when and where the communication is captured or redirected, it may also “be considered to occur at the place where the redirected contents are first heard.” Id.²

2. Geolocation Data

Courts may also authorize warrants for the disclosure of cell site records and real-time GPS monitoring if the judge determines that the warrant application’s supporting materials demonstrate probable cause. See, e.g., In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.,

² Mitselmakher contends that a recent opinion from the D.C. Circuit suggests that Rodriguez was wrongly decided. (Mitselmakher Mem. at 3–4.) However, that decision involved a warrant obtained from a judge in the District Court of the District of Columbia for a bug which was ultimately placed on a car in Baltimore (in the District of Maryland). United States v. Glover, 736 F.3d 509 (D.C. Cir. 2013). That case is distinguishable on a number of grounds; it does not change this Court’s analysis based on years of Second Circuit precedent.

460 F. Supp. 2d 448, 461 (S.D.N.Y. 2006). “While probable cause requires more than a mere suspicion of wrongdoing, its focus is on probabilities, not hard certainties. . . . It requires only such facts as make wrongdoing or the discovery of evidence thereof probable.” Walczyk v. Rio, 496 F.3d 139, 156–57 (2d Cir. 2007) (internal quotation marks and citations omitted). Thus, if an affidavit demonstrates that the discovery of evidence through GPS tracking or cell site location information is probable, the warrant may issue.³

3. Exclusionary Rule

While evidence seized in violation of the Fourth Amendment may be subject to exclusion at trial under Terry v. Ohio, 392 U.S. 1 (1968), exclusion is not automatic. See Davis v. United States, 564 U.S. 229, 248 (2011) (“Our cases have thus limited the rule’s operation to situations in which this purpose is ‘thought most efficaciously served.’” (quoting United States v. Calandra, 414 U.S. 338, 348 (1974))); see also Herring v. United States, 555 U.S. 135, 140 (2009) (“The fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies.”). At its core, the exclusionary rule is “a ‘judicially created remedy’ of [the Supreme Court’s] own making.” Davis, 564 U.S. at 238

³ Defendant Afanasyev’s reply memorandum cited a case currently pending before the Supreme Court that may address whether the Fourth Amendment permits warrantless acquisition of GPS location information; Afanasyev asked that the Court wait for the decision in that case before ruling on his motion. (See ECF No. 434 (“Reply Mem.”) at 1.) See also Carpenter v. United States, 137 S. Ct. 2211 (2017) (granting certiorari). The Court requested the Government’s response to this argument. (See ECF No. 444.)

Here, the Government had a warrant to collect the defendant’s geolocation information—a fact which defendant acknowledges. (Reply Mem. at 1.) As such, it is unlikely that a decision in Carpenter will have relevance to the instant motion. The Court will not delay its ruling based on a chance that a Supreme Court decision in a pending case might offer dicta that might be relevant.

(quoting Calandra, 414 U.S. at 348). And although the Court once “treated identification of a Fourth Amendment violation as synonymous with application of the exclusionary rule,” Arizona v. Evans, 514 U.S. 1, 13 (1995), the Court has since “abandoned the old, reflexive application of the doctrine, and imposed a more rigorous weighing of its cost and deterrence benefits,” Davis, 564 at 238 (quotation omitted). Evidence should only be suppressed “if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment.” United States v. Leon, 468 U.S. 897, 919 (1984) (quoting United States v. Peltier, 422 U.S. 531, 542 (1975)). Accordingly, the Supreme Court has held that the exclusionary rule does not apply when a search is conducted in good-faith, reasonable reliance on, inter alia, a judicially-issued warrant later held to be invalid. Leon, 468 U.S. at 922.

B. Discussion⁴

1. Intercepted Communications

Defendants here challenge the wiretap evidence on two grounds: (1) communications interceptions were unnecessary in light of the evidence obtained through normal investigative techniques (Dzhanashvili Mem.); and (2) the

⁴ Even if this Court were to find that the communications interceptions, cell site information disclosure, and GPS tracking at issue here violated the Fourth Amendment, it would still deny defendants’ suppression motions based on the officers’ good-faith reliance on the various warrants issued. See United States v. Clark, 638 F.3d 89, 99–105 (2d Cir. 2011) (applying Leon’s good-faith exception).

authorizing courts lacked territorial jurisdiction to permit the wiretaps (Mitselmakher Mem.).

As to necessity, the affidavit in support of each Title III application provided a sufficient basis for authorizing the interception. Each explained, in detail, the limits of other investigative methods and how they would not allow the FBI to adequately continue its investigation into the Shulaya Enterprise. For example, the May Affidavit stated that confidential sources are “limited in the scope of their respective access to the Shulaya Enterprise,” and specifically explained the limitations on each of five informants. (May Aff. at 59–61.)⁵ CS-2, for instance, a purported middleman in the conspiracy to transport and sell contraband cigarettes, had little visibility into the Enterprise’s purchasers for that contraband or the manner in which the contraband was disposed of. (Id. at 59.) Similarly, CS-5 was not embedded in the Shulaya Enterprise and his principal point of contact had ceased communicating with him. (Id. at 59–60.)

Relatedly, each affidavit explained that undercover operations were insufficient, as it was difficult to place someone in a prominent role within the Shulaya Enterprise; according to the May Affidavit, the defendants were been “reticent to discuss their criminal activity with outsiders and/or add superfluous members to their criminal organizations.” (Id. at 61.) For each remaining technique, including physical surveillance, pole camera surveillance, geolocation

⁵ The Court uses the May Affidavit as an example, but each of the affidavits was similarly detailed—as a result, six different judges authorized the interceptions.

information, telephone records and pen registers, grand juries and witness interviews, trash searches, and financial investigations, the FBI explained that none could adequately uncover the means and methods of the Shulaya Enterprise, or the details of the alleged criminal activity. As to search warrants and arrests, the May Affidavit explained that prematurely publicizing the existence of the investigation would “hinder the FBI’s ability to identify the source of the contraband sold” and “would seriously jeopardize the investigation.” (May Aff. at 67.)

Dzhanashvili contends that the affidavits, which detail the Shulaya Enterprise to the extent known when each was filed, demonstrate that the wiretaps were unnecessary precisely because each affidavit contained evidence obtained through means other than interception. However, the FBI need only demonstrate that “normal investigative procedures have been tried or at least considered . . . [or that] ‘normal investigative techniques had become increasingly unsuccessful’”—it need not be the case that other techniques have yielded no results. United States v. Lilla, 699 F.2d 99, 103 (2d Cir. 1983) (quoting United States v. Hinton, 543 F.2d 1002, 1011 (2d Cir. 1976)). Indeed, if that were the case, then any affidavit might suffer from a deficiency related to probable cause.

Dzhanashvili’s argument that regarding omissions in the affidavit fares no better. He contends that the December Affidavit omitted two sources of evidence—a live video feed where illegal gambling occurred and a fifth confidential source. However, omissions only trigger suppression where they were intentional, material,

or misleading. United States v. Awadallah, 349 F.3d 42, 64 (2d Cir. 2003) (citing Franks v. Delaware, 428 U.S. 154, 164–72 (1978)). Neither of the omissions here fall into these categories. First, the purported “live video feed” from surveillance cameras was disabled on November 9, 2016—before the December Order authorizing the first wiretap. (Thomas Decl. ¶ 2.) As such, the FBI could not have continued to gather information via this method, and its disclosure would not have materially impacted the authorizing judge’s decision.

Second, the omission of the fifth confidential source was immaterial, as the December Affidavit (and all those that followed) explained the limitations of confidential sources. Dzhnanashvili does not contend that CS-5 overcame those limitations (by, for example, being well-placed within the Shulaya Enterprise). And in fact, the January Affidavit explained that CS-5 was not “specifically embedded in the Shulaya Enterprise and, therefore, is not in a position to provide information sufficient to satisfy the goals of this investigation.” (January Aff. at 71.) This suggests that inclusion of this information would not have materially altered Judge Failla’s December Order.

The Court also denies Mitselmakher’s motion to suppress based on lack of territorial jurisdiction. The uncontroversial evidence is that the intercepted communications were monitored from the FBI’s wirerooms in the Southern District of New York. It is not the case, as Mitselmakher contends, that the conversation to be intercepted must occur in the jurisdiction where the judge authorized the wiretap. It is enough that the authorizing judge sits in the jurisdiction “where the

redirected contents are first heard.” Rodriguez, 968 F.2d at 136. As such, his motion to suppress the intercepted communications fails as well.

2. Geolocation Data

The GPS Affidavit demonstrated probable cause to collect geolocation information. Defendant Afanasyev submits that the GPS Affidavit failed to include the “use and aims” of the location information—but this is simply not necessary for a valid warrant to be issued. Rather, the Court must determine only that the judge who authorized the warrant acted properly based on the affidavit in support of the warrant application—that is to say, that the affidavit demonstrated the presence of probable cause. Here, the detailed GPS Affidavit specifies which phones were to be tracked and how each of the purported owners of those phones was involved in the criminal conspiracy, including in ways that involved their cellphones. (See, e.g., GPS Aff. ¶¶ 19(c), 19(i).) Because probable cause existed to support the warrant application, the warrant was validly issued. Thus, defendant’s motion to suppress the GPS monitoring data and cell site records is denied.

III. MOTION FOR DISMISSAL OF COUNT IV

A. Legal Principles

“An indictment is duplicitous if it joins two or more distinct crimes in a single count . . . [but] must be distinguished from ‘the allegation in a single count of the commission of a crime by several means.’” United States v. Aracri, 968 F.2d 1512, 1518 (2d Cir. 1992) (quoting United States v. Murray, 618 F.2d 892, 896 (2d Cir. 1980)). “A conspiracy indictment presents ‘unique issues’ in the duplicity analysis

because ‘a single agreement may encompass multiple illegal objects.’” Id. (quoting Murray, 618 F.2d at 896).

B. Discussion

Count Four of the Indictment charges nine defendants with Conspiracy to Commit Fraud Relating to Identification Documents in violation of 18 U.S.C. § 1028(f). The statute itself lists eight actions that are punishable by law; defendants are accused of committing five of those actions: 18 U.S.C. §§ 1028(a)(1), 1028(a)(2), 1028(a)(3), 1028(a)(7), and 1028(a)(8). Defendant Hovhannisyan has moved to dismiss Count IV on the ground that it is duplicitous; he maintains that each of “these subsections contain different elements, not alternative methods under which you may violate the same subsection.” (Hovhannisyan Mem. at 3.) However, Count IV properly alleges a single identity fraud conspiracy with multiple objectives. (That is to say, subsection (a) identifies the objectives, while subsection (f) identifies the overall criminal offense.) As such, the Count is not duplicitous, and the motion is DENIED.

In any case, the Court declines to address the Government’s proposal to use a special verdict form at trial to solicit a verdict to each of the various conspiratorial objects at this time. (ECF No. 421, Mem. of Law of the United States of America in Opp. to Def.’s Mots. To Suppress Evidence and for Other Relief (“Gov’t Mem.”) at 26.) This proposal may be addressed closer to trial.

IV. DISCOVERY MOTIONS

Defendants also demand discovery of routine material, including: (1) all evidence the Government intends to introduce under Fed. R. Evid. 404(b); (2) a Government witness list; (3) all exculpatory and impeachment material under Brady v. Maryland, 373 U.S. 83, 87 (1963); and (4) a bill of particulars. For the reasons stated below, defendants' discovery demands are hereby DENIED as premature.

A. Timing of Discovery

Defendant Afanasyev has requested early notice of the Government's intent to use Rule 404(b) evidence and a list of its witnesses' names and addresses. (Afanasyev Mem. at 10, 13.) This is, in effect, challenging the timing of the Government's discovery (for example, by requesting certain evidence immediately). The Court notes that the Government is under no legal obligation to provide the requested material so early. The Court declines to impose on the Government any additional discovery obligations not already contemplated by the applicable rules, absent some showing of delinquency or bad faith. The defendant has proffered no evidence to suggest that the Government will not comply with its discovery obligations in due course.

B. Discovery Obligations

Defendant Afanasyev also requests a court order "requiring the government to abide by its obligations pursuant to Brady v. United States." (ECF No. 391, Notice of Motion at 2.) To the extent defendant is requesting production of Brady material, the Government has represented that it understands its discovery obligations and that it intends to comply with such obligations. (Gov't Mem. at 36.) The defendant

has not proffered any evidence to suggest that the Government is delinquent in fulfilling its obligations, or that the Government is actively concealing evidence under Brady, Giglio, or any other rule.

Accordingly, defendant has not provided any basis upon which the Court can grant the requested relief, and there is no need to issue an order directing the Government to comply with its discovery obligations at this time.

C. Bills of Particulars

Rule 7(f) of the Federal Rules of Criminal Procedure provides that a court may direct the Government to file a bill of particulars. Fed. R. Crim. P. 7(f). However, wide ranging pre-trial discovery is not available in criminal cases. The discovery available in a criminal matter is governed by the Federal Rules of Criminal Procedure, several key cases including Brady v. Maryland, 373 U.S. 83 (1963) and Giglio v. United States, 405 U.S. 150 (1972), and the Mencks Act, 18 U.S.C. § 3500. The information defendants seek by way of bills of particulars has either already been provided or goes beyond what is necessary.

A bill of particulars is required “only where the charges of the indictment are so general that they do not advise the defendant of the specific acts of which he is accused.” United States v. Walsh, 194 F.3d 37, 47 (2d Cir. 1999) (quoting United States v. Torres, 901 F.2d 205, 234 (2d Cir. 1990)). “Acquisition of evidentiary detail is not the function of a bill of particulars.” Torres, 901 F.2d at 234 (quoting Hemphill v. United States, 392 F.2d 45, 49 (8th Cir.)). “[D]emands for particular information with respect to where, when, and with whom the Government will charge the

defendant with conspiring are routinely denied.” United States v. Trippe, 171 F. Supp. 2d 230, 240 (S.D.N.Y. 2001).

A bill of particulars is also unnecessary when the Government has produced materials in discovery concerning the witnesses and other evidence. See Walsh, 194 F.3d at 47 (“[A] bill of particulars is not necessary where the government has made sufficient disclosures concerning its evidence and witnesses by other means.”); see also United States v. Love, 859 F. Supp. 725, 738 (S.D.N.Y. 1994) (“The crucial question is whether the information sought is necessary, not whether it is helpful.” (emphasis in original)). In Torres, the Second Circuit affirmed the district court’s denial of a bill of particulars in part because the defendants were provided with considerable evidentiary detail outside of the indictment. 901 F.2d at 233–34; see also United States v. Panza, 750 F.2d 1141, 1148 (2d Cir. 1984). Thus, in determining whether to order a bill of particulars, a court must examine the totality of the information available to defendant, both through the indictment and through pre-trial discovery. United States v. Bin Laden, 92 F. Supp. 2d 225, 233 (S.D.N.Y. 2000). The purpose of the bill of particulars is to avoid prejudicial surprise at trial and give defendant sufficient information to meet the charges against him. Id. (citing Torres, 901 F.2d at 234).

In short, no provision of the Federal Rules of Criminal Procedure provide for the sort of detailed evidence supporting the charges that defendants Hovhannisyan and Afanasyev seek here. The purpose of a bill of particulars is not to provide the defense with a preview of all of the evidence that the Government intends to use at

trial. The function, rather, is to ensure that the defendants understand the nature of the charges against them so that they may fairly meet those charges.

Here, the Government has already provided defendant with significant information and materials. The Indictment and the Title III Affidavits alert the defendants of the charges against them. For example, the Indictment describes phone calls between: Shulaya and Melman (ECF No. 1, ¶¶ 11(r), 11(u), 11(w)); Shulaya and Gabisonia (id. ¶ 11(s)); Suyunov and Dzhnanashvili (id. ¶ 11(x)); and Afanasyev and Dzhnanashvili (id. ¶¶ 11(aa), 11(gg), 15(h)). Additionally, defendants have summaries or transcripts of all intercepted phone calls.

Defendants may not request bills of particulars as “general investigative tool[s],” United States v. Sindone, No. 01-cr-517, 2002 WL 48604, at *1 (S.D.N.Y. Jan. 14, 2002), and the Government need not provide the specific details requested at this time. Demands for bills of particulars need only be granted when they are necessary for a proper defense, and “demands for particular information with respect to where, when, and with whom the Government will charge the defendant with conspiring are routinely denied.” United States v. Trippe, 171 F. Supp. 2d 230, 240 (S.D.N.Y. 2001). The Court does so here.

* * *

Therefore, defendant’s discovery demands are DENIED.


V. CONCLUSION

For the reasons stated above, the Court DENIES each of the pending pre-trial motions.

The Clerk of Court is accordingly directed to terminate the motions at ECF Nos. 385, 388, 389, 391, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 413, and 420.

SO ORDERED.

Dated: New York, New York
December 20, 2017

A handwritten signature in black ink, appearing to read "K. B. Forrest", is written above a horizontal line.

KATHERINE B. FORREST
United States District Judge